

AMENDMENT IN THE NATURE OF A SUBSTITUTE
OFFERED BY MR. RUSH OF ILLINOIS

Strike all after the enacting clause and insert the
following:

1 SECTION 1. SHORT TITLE.

2 This Act may be cited as the “Data Accountability
3 and Trust Act”.

4 SEC. 2. REQUIREMENTS FOR INFORMATION SECURITY.

5 (a) GENERAL SECURITY POLICIES AND PROCE-
6 DURES.—

7 (1) REGULATIONS.—Not later than 1 year after
8 the date of enactment of this Act, the Commission
9 shall promulgate regulations under section 553 of
10 title 5, United States Code, to require each person
11 engaged in interstate commerce that owns or pos-
12 sesses data containing personal information, or con-
13 tracts to have any third party entity maintain such
14 data for such person, to establish and implement
15 policies and procedures regarding information secu-
16 rity practices for the treatment and protection of
17 personal information taking into consideration—

1 (A) the size of, and the nature, scope, and
2 complexity of the activities engaged in by, such
3 person;

4 (B) the current state of the art in adminis-
5 trative, technical, and physical safeguards for
6 protecting such information; and

7 (C) the cost of implementing such safe-
8 guards.

9 (2) REQUIREMENTS.—Such regulations shall
10 require the policies and procedures to include the
11 following:

12 (A) A security policy with respect to the
13 collection, use, sale, other dissemination, and
14 maintenance of such personal information.

15 (B) The identification of an officer or
16 other individual as the point of contact with re-
17 sponsibility for the management of information
18 security.

19 (C) A process for identifying and assessing
20 any reasonably foreseeable vulnerabilities in the
21 system or systems maintained by such person
22 that contains such data, which shall include
23 regular monitoring for a breach of security of
24 such system or systems.

1 (D) A process for taking preventive and
2 corrective action to mitigate against any
3 vulnerabilities identified in the process required
4 by subparagraph (C), which may include imple-
5 menting any changes to security practices and
6 the architecture, installation, or implementation
7 of network or operating software.

8 (E) A process for disposing of data in elec-
9 tronic form containing personal information by
10 shredding, permanently erasing, or otherwise
11 modifying the personal information contained in
12 such data to make such personal information
13 permanently unreadable or undecipherable.

14 (F) A standard method or methods for the
15 destruction of paper documents and other non-
16 electronic data containing personal information.

17 (3) TREATMENT OF ENTITIES GOVERNED BY
18 OTHER LAW.—Any person who is in compliance with
19 any other Federal law that requires such person to
20 maintain standards and safeguards for information
21 security and protection of personal information that,
22 taken as a whole and as the Commission shall deter-
23 mine in the rulemaking required under paragraph
24 (1), provide protections substantially similar to, or
25 greater than, those required under this subsection,

1 shall be deemed to be in compliance with this sub-
2 section.

3 (b) SPECIAL REQUIREMENTS FOR INFORMATION
4 BROKERS.—

5 (1) SUBMISSION OF POLICIES TO THE FTC.—

6 The regulations promulgated under subsection (a)
7 shall require each information broker to submit its
8 security policies to the Commission in conjunction
9 with a notification of a breach of security under sec-
10 tion 3 or upon request of the Commission.

11 (2) POST-BREACH AUDIT.—For any information
12 broker required to provide notification under section
13 3, the Commission may conduct audits of the infor-
14 mation security practices of such information broker,
15 or require the information broker to conduct inde-
16 pendent audits of such practices (by an independent
17 auditor who has not audited such information bro-
18 ker's security practices during the preceding 5
19 years).

20 (3) ACCURACY OF AND INDIVIDUAL ACCESS TO
21 PERSONAL INFORMATION.—

22 (A) ACCURACY.—

23 (i) IN GENERAL.—Each information
24 broker shall establish reasonable proce-
25 dures to assure the maximum possible ac-

1 curacy of the personal information it col-
2 lects, assembles, or maintains, and any
3 other information it collects, assembles, or
4 maintains that specifically identifies an in-
5 dividual, other than information which
6 merely identifies an individual's name or
7 address.

8 (ii) LIMITED EXCEPTION FOR FRAUD
9 DATABASES.—The requirement in clause
10 (i) shall not prevent the collection or main-
11 tenance of information that may be inac-
12 curate with respect to a particular indi-
13 vidual when that information is being col-
14 lected or maintained solely—

15 (I) for the purpose of indicating
16 whether there may be a discrepancy
17 or irregularity in the personal infor-
18 mation that is associated with an indi-
19 vidual; and

20 (II) to help identify, or authen-
21 ticate the identity of, an individual, or
22 to protect against or investigate fraud
23 or other unlawful conduct.

24 (B) CONSUMER ACCESS TO INFORMA-
25 TION.—

1 (i) ACCESS.—Each information broker
2 shall—

3 (I) provide to each individual
4 whose personal information it main-
5 tains, at the individual's request at
6 least 1 time per year and at no cost
7 to the individual, and after verifying
8 the identity of such individual, a
9 means for the individual to review any
10 personal information regarding such
11 individual maintained by the informa-
12 tion broker and any other information
13 maintained by the information broker
14 that specifically identifies such indi-
15 vidual, other than information which
16 merely identifies an individual's name
17 or address; and

18 (II) place a conspicuous notice on
19 its Internet website (if the informa-
20 tion broker maintains such a website)
21 instructing individuals how to request
22 access to the information required to
23 be provided under subclause (I), and,
24 as applicable, how to express a pref-
25 erence with respect to the use of per-

1 sonal information for marketing pur-
2 poses under clause (iii).

3 (ii) DISPUTED INFORMATION.—When-
4 ever an individual whose information the
5 information broker maintains makes a
6 written request disputing the accuracy of
7 any such information, the information
8 broker, after verifying the identity of the
9 individual making such request and unless
10 there are reasonable grounds to believe
11 such request is frivolous or irrelevant,
12 shall—

13 (I) correct any inaccuracy; or

14 (II)(aa) in the case of informa-
15 tion that is public record information,
16 inform the individual of the source of
17 the information, and, if reasonably
18 available, where a request for correc-
19 tion may be directed and, if the indi-
20 vidual provides proof that the public
21 record has been corrected or that the
22 information broker was reporting the
23 information incorrectly, correct the in-
24 accuracy in the information broker's
25 records; or

1 (bb) in the case of information
2 that is non-public information, note
3 the information that is disputed, in-
4 cluding the individual's statement dis-
5 puting such information, and take
6 reasonable steps to independently
7 verify such information under the pro-
8 cedures outlined in subparagraph (A)
9 if such information can be independ-
10 ently verified.

11 (iii) ALTERNATIVE PROCEDURE FOR
12 CERTAIN MARKETING INFORMATION.—In
13 accordance with regulations issued under
14 clause (v), an information broker that
15 maintains any information described in
16 clause (i) which is used, shared, or sold by
17 such information broker for marketing
18 purposes, may, in lieu of complying with
19 the access and dispute requirements set
20 forth in clauses (i) and (ii), provide each
21 individual whose information it maintains
22 with a reasonable means of expressing a
23 preference not to have his or her informa-
24 tion used for such purposes. If the indi-
25 vidual expresses such a preference, the in-

1 formation broker may not use, share, or
2 sell the individual's information for mar-
3 keting purposes.

4 (iv) LIMITATIONS.—An information
5 broker may limit the access to information
6 required under clause (i)(I) and is not re-
7 quired to provide notice to individuals as
8 required under clause (i)(II) in the fol-
9 lowing circumstances:

10 (I) If access of the individual to
11 the information is limited by law or
12 legally recognized privilege.

13 (II) If the information is used for
14 a legitimate governmental or fraud
15 prevention purpose that would be
16 compromised by such access.

17 (III) If the information consists
18 of a published media record, unless
19 that record has been included in a re-
20 port about an individual shared with a
21 third party.

22 (v) RULEMAKING.—Not later than 1
23 year after the date of the enactment of this
24 Act, the Commission shall promulgate reg-
25 ulations under section 553 of title 5,

1 United States Code, to carry out this para-
2 graph and to facilitate the purposes of this
3 Act. In addition, the Commission shall
4 issue regulations, as necessary, under sec-
5 tion 553 of title 5, United States Code, on
6 the scope of the application of the limita-
7 tions in clause (iv), including any addi-
8 tional circumstances in which an informa-
9 tion broker may limit access to information
10 under such clause that the Commission de-
11 termines to be appropriate.

12 (C) FCRA REGULATED PERSONS.—Any
13 information broker who is engaged in activities
14 subject to the Fair Credit Reporting Act and
15 who is in compliance with sections 609, 610,
16 and 611 of such Act (15 U.S.C. 1681g; 1681h;
17 1681i) with respect to information subject to
18 such Act, shall be deemed to be in compliance
19 with this paragraph with respect to such infor-
20 mation.

21 (4) REQUIREMENT OF AUDIT LOG OF ACCESSED
22 AND TRANSMITTED INFORMATION.—Not later than
23 1 year after the date of the enactment of this Act,
24 the Commission shall promulgate regulations under
25 section 553 of title 5, United States Code, to require

1 information brokers to establish measures which fa-
2 cilitate the auditing or retracing of any internal or
3 external access to, or transmissions of, any data con-
4 taining personal information collected, assembled, or
5 maintained by such information broker.

6 (5) PROHIBITION ON PRETEXTING BY INFOR-
7 MATION BROKERS.—

8 (A) PROHIBITION ON OBTAINING PER-
9 SONAL INFORMATION BY FALSE PRETENSES.—

10 It shall be unlawful for an information broker
11 to obtain or attempt to obtain, or cause to be
12 disclosed or attempt to cause to be disclosed to
13 any person, personal information or any other
14 information relating to any person by—

15 (i) making a false, fictitious, or fraud-
16 ulent statement or representation to any
17 person; or

18 (ii) providing any document or other
19 information to any person that the infor-
20 mation broker knows or should know to be
21 forged, counterfeit, lost, stolen, or fraudu-
22 lently obtained, or to contain a false, ficti-
23 tious, or fraudulent statement or represen-
24 tation.

1 (B) PROHIBITION ON SOLICITATION TO
2 OBTAIN PERSONAL INFORMATION UNDER FALSE
3 PRETENSES.—It shall be unlawful for an infor-
4 mation broker to request a person to obtain
5 personal information or any other information
6 relating to any other person, if the information
7 broker knew or should have known that the per-
8 son to whom such a request is made will obtain
9 or attempt to obtain such information in the
10 manner described in subparagraph (A).

11 (c) EXEMPTION FOR CERTAIN SERVICE PRO-
12 VIDERS.—Nothing in this section shall apply to a service
13 provider for any electronic communication by a third party
14 that is transmitted, routed, or stored in intermediate or
15 transient storage by such service provider.

16 **SEC. 3. NOTIFICATION OF INFORMATION SECURITY**
17 **BREACH.**

18 (a) NATIONWIDE NOTIFICATION.—Any person en-
19 gaged in interstate commerce that owns or possesses data
20 in electronic form containing personal information shall,
21 following the discovery of a breach of security of the sys-
22 tem maintained by such person that contains such data—
23 (1) notify each individual who is a citizen or
24 resident of the United States whose personal infor-

1 mation was acquired or accessed as a result of such
2 a breach of security; and

3 (2) notify the Commission.

4 (b) SPECIAL NOTIFICATION REQUIREMENTS.—

5 (1) THIRD PARTY AGENTS.—In the event of a
6 breach of security by any third party entity that has
7 been contracted to maintain or process data in elec-
8 tronic form containing personal information on be-
9 half of any other person who owns or possesses such
10 data, such third party entity shall be required to no-
11 tify such person of the breach of security. Upon re-
12 ceiving such notification from such third party, such
13 person shall provide the notification required under
14 subsection (a).

15 (2) SERVICE PROVIDERS.—If a service provider
16 becomes aware of a breach of security of data in
17 electronic form containing personal information that
18 is owned or possessed by another person that con-
19 nects to or uses a system or network provided by the
20 service provider for the purpose of transmitting,
21 routing, or providing intermediate or transient stor-
22 age of such data, such service provider shall be re-
23 quired to notify of such a breach of security only the
24 person who initiated such connection, transmission,
25 routing, or storage if such person can be reasonably

1 identified. Upon receiving such notification from a
2 service provider, such person shall provide the notifi-
3 cation required under subsection (a).

4 (3) COORDINATION OF NOTIFICATION WITH
5 CONSUMER REPORTING AGENCIES.—If a person is
6 required to provide notification to more than 5,000
7 individuals under subsection (a)(1), the person shall
8 also notify the major consumer reporting agencies of
9 the timing and distribution of the notices. Such no-
10 tice shall be given to the consumer reporting agen-
11 cies without unreasonable delay and, if it will not
12 delay notice to the affected individuals, prior to the
13 distribution of notices to the affected individuals.

14 (c) TIMELINESS OF NOTIFICATION.—

15 (1) IN GENERAL.—Unless subject to a delay au-
16 thorized under paragraph (2), a notification required
17 under subsection (a) shall be made not later than 45
18 days following the discovery of a breach of security,
19 unless the person providing notice can show that
20 providing notice within such a time frame is not fea-
21 sible due to extraordinary circumstances necessary
22 to prevent further breach or unauthorized disclo-
23 sures, and reasonably restore the integrity of the
24 data system, in which case such notification shall be
25 made as promptly as possible.

1 (2) DELAY OF NOTIFICATION AUTHORIZED FOR
2 LAW ENFORCEMENT OR NATIONAL SECURITY PUR-
3 POSES.—

4 (A) LAW ENFORCEMENT.—If a Federal,
5 State, or local law enforcement agency deter-
6 mines that the notification required under this
7 section would impede a civil or criminal inves-
8 tigation, such notification shall be delayed upon
9 the written request of the law enforcement
10 agency for 30 days or such lesser period of time
11 which the law enforcement agency determines is
12 reasonably necessary and requests in writing. A
13 law enforcement agency may, by a subsequent
14 written request, revoke such delay or extend the
15 period of time set forth in the original request
16 made under this paragraph if further delay is
17 necessary.

18 (B) NATIONAL SECURITY.—If a Federal
19 national security agency or homeland security
20 agency determines that the notification required
21 under this section would threaten national or
22 homeland security, such notification may be de-
23 layed for a period of time which the national se-
24 curity agency or homeland security agency de-
25 termines is reasonably necessary and requests

1 in writing. A Federal national security agency
2 or homeland security agency may revoke such
3 delay or extend the period of time set forth in
4 the original request made under this paragraph
5 by a subsequent written request if further delay
6 is necessary.

7 (d) METHOD AND CONTENT OF NOTIFICATION.—

8 (1) DIRECT NOTIFICATION.—

9 (A) METHOD OF NOTIFICATION.—A person
10 required to provide notification to individuals
11 under subsection (a)(1) shall be in compliance
12 with such requirement if the person provides
13 conspicuous and clearly identified notification
14 by one of the following methods (provided the
15 selected method can reasonably be expected to
16 reach the intended individual):

17 (i) Written notification.

18 (ii) Notification by email or other
19 electronic means, if—

20 (I) the person's primary method
21 of communication with the individual
22 is by email or such other electronic
23 means; or

24 (II) the individual has consented
25 to receive such notification and the

1 notification is provided in a manner
2 that is consistent with the provisions
3 permitting electronic transmission of
4 notices under section 101 of the Elec-
5 tronic Signatures in Global and Na-
6 tional Commerce Act (15 U.S.C.
7 7001).

8 (B) CONTENT OF NOTIFICATION.—Regard-
9 less of the method by which notification is pro-
10 vided to an individual under subparagraph (A),
11 such notification shall include—

12 (i) a description of the personal infor-
13 mation that was acquired or accessed by
14 an unauthorized person;

15 (ii) a telephone number that the indi-
16 vidual may use, at no cost to such indi-
17 vidual, to contact the person to inquire
18 about the breach of security or the infor-
19 mation the person maintained about that
20 individual;

21 (iii) notice that the individual is enti-
22 tled to receive, at no cost to such indi-
23 vidual, consumer credit reports on a quar-
24 terly basis for a period of 2 years, or credit
25 monitoring or other service that enables

1 consumers to detect the misuse of their
2 personal information for a period of 2
3 years, and instructions to the individual on
4 requesting such reports or service from the
5 person, except when the only information
6 which has been the subject of the security
7 breach is the individual's first name or ini-
8 tial and last name, or address, or phone
9 number, in combination with a credit or
10 debit card number, and any required secu-
11 rity code;

12 (iv) the toll-free contact telephone
13 numbers and addresses for the major con-
14 sumer reporting agencies; and

15 (v) a toll-free telephone number and
16 Internet website address for the Commis-
17 sion whereby the individual may obtain in-
18 formation regarding identity theft.

19 (2) SUBSTITUTE NOTIFICATION.—

20 (A) CIRCUMSTANCES GIVING RISE TO SUB-
21 STITUTE NOTIFICATION.—A person required to
22 provide notification to individuals under sub-
23 section (a)(1) may provide substitute notifica-
24 tion in lieu of the direct notification required by
25 paragraph (1) if the person owns or possesses

1 data in electronic form containing personal in-
2 formation of fewer than 1,000 individuals and
3 such direct notification is not feasible due to—

4 (i) excessive cost to the person re-
5 quired to provide such notification relative
6 to the resources of such person, as deter-
7 mined in accordance with the regulations
8 issued by the Commission under paragraph
9 (3)(A); or

10 (ii) lack of sufficient contact informa-
11 tion for the individual required to be noti-
12 fied.

13 (B) FORM OF SUBSTITUTE NOTIFICA-
14 TION.—Such substitute notification shall in-
15 clude—

16 (i) email notification to the extent
17 that the person has email addresses of in-
18 dividuals to whom it is required to provide
19 notification under subsection (a)(1);

20 (ii) a conspicuous notice on the Inter-
21 net website of the person (if such person
22 maintains such a website); and

23 (iii) notification in print and to broad-
24 cast media, including major media in met-
25 ropolitan and rural areas where the indi-

1 individuals whose personal information was ac-
2 quired reside.

3 (C) CONTENT OF SUBSTITUTE NOTICE.—

4 Each form of substitute notice under this para-
5 graph shall include—

6 (i) notice that individuals whose per-
7 sonal information is included in the breach
8 of security are entitled to receive, at no
9 cost to the individuals, consumer credit re-
10 ports on a quarterly basis for a period of
11 2 years, or credit monitoring or other serv-
12 ice that enables consumers to detect the
13 misuse of their personal information for a
14 period of 2 years, and instructions on re-
15 questing such reports or service from the
16 person, except when the only information
17 which has been the subject of the security
18 breach is the individual's first name or ini-
19 tial and last name, or address, or phone
20 number, in combination with a credit or
21 debit card number, and any required secu-
22 rity code; and

23 (ii) a telephone number by which an
24 individual can, at no cost to such indi-
25 vidual, learn whether that individual's per-

1 sonal information is included in the breach
2 of security.

3 (3) REGULATIONS AND GUIDANCE.—

4 (A) REGULATIONS.—Not later than 1 year
5 after the date of enactment of this Act, the
6 Commission shall, by regulation under section
7 553 of title 5, United States Code, establish cri-
8 teria for determining circumstances under
9 which substitute notification may be provided
10 under paragraph (2), including criteria for de-
11 termining if notification under paragraph (1) is
12 not feasible due to excessive costs to the person
13 required to provide such notification relative to
14 the resources of such person. Such regulations
15 may also identify other circumstances where
16 substitute notification would be appropriate for
17 any person, including circumstances under
18 which the cost of providing notification exceeds
19 the benefits to consumers.

20 (B) GUIDANCE.—In addition, the Commis-
21 sion shall provide and publish general guidance
22 with respect to compliance with this subsection.
23 Such guidance shall include—

1 (i) a description of written or email
2 notification that complies with the require-
3 ments of paragraph (1); and

4 (ii) guidance on the content of sub-
5 stitute notification under paragraph (2),
6 including the extent of notification to print
7 and broadcast media that complies with
8 the requirements of such paragraph.

9 (e) OTHER OBLIGATIONS FOLLOWING BREACH.—

10 (1) IN GENERAL.—A person required to provide
11 notification under subsection (a) shall, upon request
12 of an individual whose personal information was in-
13 cluded in the breach of security, provide or arrange
14 for the provision of, to each such individual and at
15 no cost to such individual—

16 (A) consumer credit reports from at least
17 one of the major consumer reporting agencies
18 beginning not later than 60 days following the
19 individual's request and continuing on a quar-
20 terly basis for a period of 2 years thereafter; or

21 (B) a credit monitoring or other service
22 that enables consumers to detect the misuse of
23 their personal information, beginning not later
24 than 60 days following the individual's request
25 and continuing for a period of 2 years.

1 (2) LIMITATION.—This subsection shall not
2 apply if the only personal information which has
3 been the subject of the security breach is the individ-
4 ual's first name or initial and last name, or address,
5 or phone number, in combination with a credit or
6 debit card number, and any required security code.

7 (3) RULEMAKING.—As part of the Commis-
8 sion's rulemaking described in subsection (d)(3), the
9 Commission shall determine the circumstances under
10 which a person required to provide notification
11 under subsection (a)(1) shall provide or arrange for
12 the provision of free consumer credit reports or cred-
13 it monitoring or other service to affected individuals.

14 (f) EXEMPTION.—

15 (1) GENERAL EXEMPTION.—A person shall be
16 exempt from the requirements under this section if,
17 following a breach of security, such person deter-
18 mines that there is no reasonable risk of identity
19 theft, fraud, or other unlawful conduct.

20 (2) PRESUMPTION.—

21 (A) IN GENERAL.—If the data in electronic
22 form containing personal information is ren-
23 dered unusable, unreadable, or indecipherable
24 through encryption or other security technology
25 or methodology (if the method of encryption or

1 such other technology or methodology is gen-
2 erally accepted by experts in the information se-
3 curity field), there shall be a presumption that
4 no reasonable risk of identity theft, fraud, or
5 other unlawful conduct exists following a breach
6 of security of such data. Any such presumption
7 may be rebutted by facts demonstrating that
8 the encryption or other security technologies or
9 methodologies in a specific case, have been or
10 are reasonably likely to be compromised.

11 (B) METHODOLOGIES OR TECH-
12 NOLOGIES.—Not later than 1 year after the
13 date of the enactment of this Act and bian-
14 nually thereafter, the Commission shall issue
15 rules (pursuant to section 553 of title 5, United
16 States Code) or guidance to identify security
17 methodologies or technologies which render data
18 in electronic form unusable, unreadable, or in-
19 decipherable, that shall, if applied to such data,
20 establish a presumption that no reasonable risk
21 of identity theft, fraud, or other unlawful con-
22 duct exists following a breach of security of
23 such data. Any such presumption may be rebut-
24 ted by facts demonstrating that any such meth-
25 odology or technology in a specific case has

1 been or is reasonably likely to be compromised.
2 In issuing such rules or guidance, the Commis-
3 sion shall consult with relevant industries, con-
4 sumer organizations, and data security and
5 identity theft prevention experts and established
6 standards setting bodies.

7 (3) FTC GUIDANCE.—Not later than 1 year
8 after the date of the enactment of this Act the Com-
9 mission shall issue guidance regarding the applica-
10 tion of the exemption in paragraph (1).

11 (g) WEBSITE NOTICE OF FEDERAL TRADE COMMIS-
12 SION.—If the Commission, upon receiving notification of
13 any breach of security that is reported to the Commission
14 under subsection (a)(2), finds that notification of such a
15 breach of security via the Commission’s Internet website
16 would be in the public interest or for the protection of
17 consumers, the Commission shall place such a notice in
18 a clear and conspicuous location on its Internet website.

19 (h) FTC STUDY ON NOTIFICATION IN LANGUAGES
20 IN ADDITION TO ENGLISH.—Not later than 1 year after
21 the date of enactment of this Act, the Commission shall
22 conduct a study on the practicality and cost effectiveness
23 of requiring the notification required by subsection (d)(1)
24 to be provided in a language in addition to English to indi-
25 viduals known to speak only such other language.

1 (i) GENERAL RULEMAKING AUTHORITY.—The Com-
2 mission may promulgate regulations necessary under sec-
3 tion 553 of title 5, United States Code, to effectively en-
4 force the requirements of this section.

5 (j) TREATMENT OF PERSONS GOVERNED BY OTHER
6 LAW.—A person who is in compliance with any other Fed-
7 eral law that requires such person to provide notification
8 to individuals following a breach of security, and that,
9 taken as a whole, provides protections substantially similar
10 to, or greater than, those required under this section, as
11 the Commission shall determine by rule (under section
12 553 of title 5, United States Code), shall be deemed to
13 be in compliance with this section.

14 **SEC. 4. APPLICATION AND ENFORCEMENT.**

15 (a) GENERAL APPLICATION.—The requirements of
16 sections 2 and 3 shall only apply to those persons, partner-
17 ships, or corporations over which the Commission has au-
18 thority pursuant to section 5(a)(2) of the Federal Trade
19 Commission Act (15 U.S.C. 45(a)(2)).

20 (b) ENFORCEMENT BY THE FEDERAL TRADE COM-
21 MISSION.—

22 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
23 TICES.—A violation of section 2 or 3 shall be treated
24 as an unfair and deceptive act or practice in viola-
25 tion of a regulation under section 18(a)(1)(B) of the

1 Federal Trade Commission Act (15 U.S.C.
2 57a(a)(1)(B)) regarding unfair or deceptive acts or
3 practices.

4 (2) POWERS OF COMMISSION.—The Commis-
5 sion shall enforce this Act in the same manner, by
6 the same means, and with the same jurisdiction,
7 powers, and duties as though all applicable terms
8 and provisions of the Federal Trade Commission Act
9 (15 U.S.C. 41 et seq.) were incorporated into and
10 made a part of this Act. Any person who violates
11 such regulations shall be subject to the penalties and
12 entitled to the privileges and immunities provided in
13 that Act.

14 (3) LIMITATION.—In promulgating rules under
15 this Act, the Commission shall not require the de-
16 ployment or use of any specific products or tech-
17 nologies, including any specific computer software or
18 hardware.

19 (c) ENFORCEMENT BY STATE ATTORNEYS GEN-
20 ERAL.—

21 (1) CIVIL ACTION.—In any case in which the
22 attorney general of a State, or an official or agency
23 of a State, has reason to believe that an interest of
24 the residents of that State has been or is threatened
25 or adversely affected by any person who violates sec-

1 tion 2 or 3 of this Act, the attorney general, official,
2 or agency of the State, as *parens patriae*, may bring
3 a civil action on behalf of the residents of the State
4 in a district court of the United States of appro-
5 priate jurisdiction—

6 (A) to enjoin further violation of such sec-
7 tion by the defendant;

8 (B) to compel compliance with such sec-
9 tion; or

10 (C) to obtain civil penalties in the amount
11 determined under paragraph (2).

12 (2) CIVIL PENALTIES.—

13 (A) CALCULATION.—

14 (i) TREATMENT OF VIOLATIONS OF
15 SECTION 2.—For purposes of paragraph
16 (1)(C) with regard to a violation of section
17 2, the amount determined under this para-
18 graph is the amount calculated by multi-
19 plying the number of days that a person is
20 not in compliance with such section by an
21 amount not greater than \$11,000.

22 (ii) TREATMENT OF VIOLATIONS OF
23 SECTION 3.—For purposes of paragraph
24 (1)(C) with regard to a violation of section
25 3, the amount determined under this para-

1 graph is the amount calculated by multi-
2 plying the number of violations of such
3 section by an amount not greater than
4 \$11,000. Each failure to send notification
5 as required under section 3 to a resident of
6 the State shall be treated as a separate
7 violation.

8 (B) ADJUSTMENT FOR INFLATION.—Be-
9 ginning on the date that the Consumer Price
10 Index is first published by the Bureau of Labor
11 Statistics that is after 1 year after the date of
12 enactment of this Act, and each year thereafter,
13 the amounts specified in clauses (i) and (ii) of
14 subparagraph (A) shall be increased by the per-
15 centage increase in the Consumer Price Index
16 published on that date from the Consumer
17 Price Index published the previous year.

18 (C) MAXIMUM TOTAL LIABILITY.—Not-
19 withstanding the number of actions which may
20 be brought against a person under this sub-
21 section, the maximum civil penalty for which
22 any person may be liable under this subsection
23 shall not exceed—

24 (i) \$5,000,000 for each violation of
25 section 2; and

1 (ii) \$5,000,000 for all violations of
2 section 3 resulting from a single breach of
3 security.

4 (3) INTERVENTION BY THE FTC.—

5 (A) NOTICE AND INTERVENTION.—The
6 State shall provide prior written notice of any
7 action under paragraph (1) to the Commission
8 and provide the Commission with a copy of its
9 complaint, except in any case in which such
10 prior notice is not feasible, in which case the
11 State shall serve such notice immediately upon
12 instituting such action. The Commission shall
13 have the right—

14 (i) to intervene in the action;

15 (ii) upon so intervening, to be heard
16 on all matters arising therein; and

17 (iii) to file petitions for appeal.

18 (B) LIMITATION ON STATE ACTION WHILE
19 FEDERAL ACTION IS PENDING.—If the Commis-
20 sion has instituted a civil action for violation of
21 this Act, no State attorney general, or official
22 or agency of a State, may bring an action under
23 this subsection during the pendency of that ac-
24 tion against any defendant named in the com-

1 plaint of the Commission for any violation of
2 this Act alleged in the complaint.

3 (4) CONSTRUCTION.—For purposes of bringing
4 any civil action under paragraph (1), nothing in this
5 Act shall be construed to prevent an attorney gen-
6 eral of a State from exercising the powers conferred
7 on the attorney general by the laws of that State
8 to—

9 (A) conduct investigations;

10 (B) administer oaths or affirmations; or

11 (C) compel the attendance of witnesses or
12 the production of documentary and other evi-
13 dence.

14 (d) AFFIRMATIVE DEFENSE FOR A VIOLATION OF
15 SECTION 3.—

16 (1) IN GENERAL.—It shall be an affirmative de-
17 fense to an enforcement action brought under sub-
18 section (b), or a civil action brought under sub-
19 section (c), based on a violation of section 3, that all
20 of the personal information contained in the data in
21 electronic form that was acquired or accessed as a
22 result of a breach of security of the defendant is
23 public record information that is lawfully made
24 available to the general public from Federal, State,

1 or local government records and was acquired by the
2 defendant from such records.

3 (2) NO EFFECT ON OTHER REQUIREMENTS.—
4 Nothing in this subsection shall be construed to ex-
5 empt any person from the requirement to notify the
6 Commission of a breach of security as required
7 under section 3(a).

8 **SEC. 5. DEFINITIONS.**

9 In this Act, the following definitions apply:

10 (1) BREACH OF SECURITY.—The term “breach
11 of security” means the unauthorized acquisition of
12 data in electronic form containing personal informa-
13 tion.

14 (2) COMMISSION.—The term “Commission”
15 means the Federal Trade Commission.

16 (3) CONSUMER REPORTING AGENCY.—The term
17 “consumer reporting agency” has the meaning given
18 the term “consumer reporting agency that compiles
19 and maintains files on consumers on a nationwide
20 basis” in section 603(p) of the Fair Credit Report-
21 ing Act (15 U.S.C. 1681a(p)).

22 (4) DATA IN ELECTRONIC FORM.—The term
23 “data in electronic form” means any data stored
24 electronically or digitally on any computer system or

1 other database and includes recordable tapes and
2 other mass storage devices.

3 (5) ENCRYPTION.—The term “encryption”
4 means the protection of data in electronic form in
5 storage or in transit using an encryption technology
6 that has been adopted by an established standards
7 setting body which renders such data indecipherable
8 in the absence of associated cryptographic keys nec-
9 essary to enable decryption of such data. Such
10 encryption must include appropriate management
11 and safeguards of such keys to protect the integrity
12 of the encryption.

13 (6) IDENTITY THEFT.—The term “identity
14 theft” means the unauthorized use of another per-
15 son’s personal information for the purpose of engag-
16 ing in commercial transactions under the name of
17 such other person.

18 (7) INFORMATION BROKER.—The term “infor-
19 mation broker”—

20 (A) means a commercial entity whose busi-
21 ness is to collect, assemble, or maintain per-
22 sonal information concerning individuals who
23 are not current or former customers of such en-
24 tity in order to sell such information or provide
25 access to such information to any nonaffiliated

1 third party in exchange for consideration,
2 whether such collection, assembly, or mainte-
3 nance of personal information is performed by
4 the information broker directly, or by contract
5 or subcontract with any other entity; and

6 (B) does not include a commercial entity to
7 the extent that such entity processes informa-
8 tion collected by and received from a non-
9 affiliated third party concerning individuals who
10 are current or former customers or employees
11 of such third party to enable such third party
12 to (1) provide benefits for its employees or (2)
13 directly transact business with its customers.

14 (8) PERSONAL INFORMATION.—

15 (A) DEFINITION.—The term “personal in-
16 formation” means an individual’s first name or
17 initial and last name, or address, or phone
18 number, in combination with any 1 or more of
19 the following data elements for that individual:

20 (i) Social Security number.

21 (ii) Driver’s license number, passport
22 number, military identification number, or
23 other similar number issued on a govern-
24 ment document used to verify identity.

1 (iii) Financial account number, or
2 credit or debit card number, and any re-
3 quired security code, access code, or pass-
4 word that is necessary to permit access to
5 an individual's financial account.

6 (B) MODIFIED DEFINITION BY RULE-
7 MAKING.—The Commission may, by rule pro-
8 mulgated under section 553 of title 5, United
9 States Code, modify the definition of “personal
10 information” under subparagraph (A)—

11 (i) for the purpose of section 2 to the
12 extent that such modification will not un-
13 reasonably impede interstate commerce,
14 and will accomplish the purposes of this
15 Act; or

16 (ii) for the purpose of section 3, to the
17 extent that such modification is necessary
18 to accommodate changes in technology or
19 practices, will not unreasonably impede
20 interstate commerce, and will accomplish
21 the purposes of this Act.

22 (9) PUBLIC RECORD INFORMATION.—The term
23 “public record information” means information
24 about an individual which has been obtained origi-
25 nally from records of a Federal, State, or local gov-

1 ernment entity that are available for public inspec-
2 tion.

3 (10) NON-PUBLIC INFORMATION.—The term
4 “non-public information” means information about
5 an individual that is of a private nature and neither
6 available to the general public nor obtained from a
7 public record.

8 (11) SERVICE PROVIDER.—The term “service
9 provider” means an entity that provides to a user
10 transmission, routing, intermediate and transient
11 storage, or connections to its system or network, for
12 electronic communications, between or among points
13 specified by such user of material of the user’s
14 choosing, without modification to the content of the
15 material as sent or received. Any such entity shall
16 be treated as a service provider under this Act only
17 to the extent that it is engaged in the provision of
18 such transmission, routing, intermediate and tran-
19 sient storage or connections.

20 **SEC. 6. EFFECT ON OTHER LAWS.**

21 (a) PREEMPTION OF STATE INFORMATION SECURITY
22 LAWS.—This Act supersedes any provision of a statute,
23 regulation, or rule of a State or political subdivision of
24 a State, with respect to those entities covered by the regu-
25 lations issued pursuant to this Act, that expressly—

1 (1) requires information security practices and
2 treatment of data containing personal information
3 similar to any of those required under section 2; and

4 (2) requires notification to individuals of a
5 breach of security resulting in unauthorized access
6 to or acquisition of data in electronic form con-
7 taining personal information.

8 (b) ADDITIONAL PREEMPTION.—

9 (1) IN GENERAL.—No person other than a per-
10 son specified in section 4(c) may bring a civil action
11 under the laws of any State if such action is pre-
12 mised in whole or in part upon the defendant vio-
13 lating any provision of this Act.

14 (2) PROTECTION OF CONSUMER PROTECTION
15 LAWS.—This subsection shall not be construed to
16 limit the enforcement of any State consumer protec-
17 tion law by an attorney general of a State.

18 (c) PROTECTION OF CERTAIN STATE LAWS.—This
19 Act shall not be construed to preempt the applicability
20 of—

21 (1) State trespass, contract, or tort law; or

22 (2) other State laws to the extent that those
23 laws relate to acts of fraud.

24 (d) PRESERVATION OF FTC AUTHORITY.—Nothing
25 in this Act may be construed in any way to limit or affect

1 the Commission's authority under any other provision of
2 law.

3 **SEC. 7. EFFECTIVE DATE.**

4 This Act shall take effect 1 year after the date of
5 enactment of this Act.

6 **SEC. 8. AUTHORIZATION OF APPROPRIATIONS.**

7 There is authorized to be appropriated to the Com-
8 mission \$1,000,000 for each of fiscal years 2016 through
9 2020 to carry out this Act.

